



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,167	09/14/2000	Anton Enterrottacher	P00.0637	5982

24573 7590 06/10/2005  
BELL, BOYD & LLOYD, LLC  
PO BOX 1135  
CHICAGO, IL 60690-1135

EXAMINER

DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/646,167

Applicant(s)

ENTERROTTACHER ET AL.

Examiner

Zachary A. Davis

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 24 March 2005.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 4,6-8 and 10-12 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 4,6-8 and 10-12 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. An amendment was received on 24 March 2005. Claims 4, 7, 8, and 10 have been amended. Claims 5 and 9 have been canceled. No new claims have been added. Claims 4, 6-8, and 10-12 are currently pending in the present application.

### ***Response to Arguments***

2. Applicant's arguments filed 24 March 2005 have been fully considered but they are not persuasive.

Claims 4-6, 8, and 12 were rejected under 35 U.S.C. 102(e) as being anticipated by Mittra, US Patent 5748736. Claims 7 and 9-11 were rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra in view of Schneier, *Applied Cryptography*.

Regarding the rejections under 35 U.S.C. 102(e), Applicant states that Mittra is silent regarding the type of signature or encryption used in the application; however, Applicant goes on to state that Mittra does teach the use of public key algorithms, citing column 9, line 48-column 10, line 62. Applicant argues that Mittra does not encrypt the signature using a private/public key; however, the Examiner believes that Mittra does disclose that public key algorithms that have a signature function can be used (see column 10, line 62-column 11, line 3, where, for example, signatures can be performed according to the ElGamal or RSA algorithms). Applicant additionally states that the authentication performed by Mittra is "based on a certificate assigned to each member

of the communication group” and that “the certificate is signed with a general-purpose signature” (see page 8 of the present response). The Examiner agrees with this characterization, and notes that the “certificate assigned to each member” is therefore “device-specific” as claimed and that the “general-purpose signature” is therefore “group-specific” as claimed (see Mittra, column 11, lines 35-41). Applicant further argues that the disclosure of Mittra “requires that a specific key must be exclusively chosen for encrypting the data” (page 8 of the present response); however, the Examiner notes that this key may be the group key (see Mittra, column 9, lines 63-66).

Applicant therefore argues that Mittra does not disclose “assigning each key device a group-specific public key, wherein a group comprised of a limited total number of key devices; assigning each key device a group-specific signature of the device-specific certificate” and “establishing a link between at least two key devices transmitting a corresponding device-specific certificate and a corresponding device-specific signature from one of the key devices to another one of the key devices, wherein the other one of the key devices verifying authenticity of the corresponding device-specific certificate” as claimed. However, the Examiner believes that Mittra does indeed disclose such limitations. Specifically, the Examiner believes that Mittra discloses assigning each device a group specific public key, where the group includes a limited total number of devices (column 8, lines 15-35; column 9, lines 56-58); assigning each device a group-specific signature of the device-specific certificate (column 11, lines 35-39); establishing a link between at least two key devices transmitting a corresponding device-specific certificate and signature from one of the devices to

another (column 11, lines 39-41); and the other device verifying the authenticity of the corresponding certificate (column 11, lines 8-10).

Regarding the rejections under 35 U.S.C. 103(a), in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Schneier does not disclose the transmission of a certificate and corresponding key. However, Schneier was not relied upon to teach the limitations relating to the device-specific certificate; rather, Mittra was relied upon to disclose those limitations, as set forth above. Applicant further argues that Schneier "does not disclose the verification relationship discussed above" (page 8 of the present response). The Examiner respectfully disagrees. Schneier discloses that a digital signature is formed by encrypting a document with a private key and that the signature is verified by decrypting the encrypted document with the corresponding public key (see page 37, where the "basic protocol" is described"). This corresponds exactly to the relationship recited in Claims 7, 8, and 10, in which sAD is the secret or private key, pAD is the public key, and Z(A) is the document that is being signed and verified.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to combine the references is as stated in the previous Office action, namely to allow the signature to be authentic, unforgeable, and usable only once (see Schneier, page 37). Applicant further argues that the disclosure of Schneier obviates the usage of the GSC of Mittra. The Examiner respectfully disagrees, and notes that Schneier states that a trusted third party ("Trent") is not needed either to sign or verify signatures, but is still needed to certify the public keys (see Schneier, page 37). It is further noted that the GSC of Mittra provides certificates to the group members and signs the certificates (column 11, lines 35-41); however, the GSC does not perform signatures for messages sent between the group members (column 11, lines 42-43). This is not analogous to Schneier's statement that digital signatures do not require the trusted third party.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

### ***Claim Objections***

3. Claims 11 and 12 are objected to because of the following informalities:

Claim 11 recites "The method according claim 10". It appears that this is intended to recite "The method according to claim 10". Similarly, it appears that, in Claim 12, "The method according claim 8" is intended to read "The method according to claim 8".

Appropriate correction is required.

4. Applicant is advised that should claim 8 be found allowable, claim 10 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 4 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by Mittra, US Patent 5748736.

In reference to Claim 4, Mittra discloses a method for authenticating key devices, in which each key device is assigned a device-specific certificate (column 11, lines 35-38), including the steps of assigning each device a group-specific public key, where the group is comprised of a limited total number of key devices (column 8, lines 15-35; column 9, lines 56-58); assigning each key device a group-specific signature of its certificate (column 11, lines 35-39), where the group-specific public key and the group-specific signature of the device-specific certificate are allocated to each key device during a first initialization (column 8, lines 33-35); establishing a link between at least two key devices; and transmitting a corresponding device-specific certificate and public key from one of the key devices to another of the key devices (column 11, lines 35-41, where the signed certificates are sent along with any message sent to the group), where the other key device verifies authenticity of the corresponding device-specific certificate using the corresponding public key (column 11, lines 8-10).

In reference to Claim 6, Mittra further discloses that each key device is compared with a stored list of approved key devices (column 7, lines 52-57).



***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 7, 8, and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra in view of Schneier, *Applied Cryptography*.

In reference to Claim 7, Mittra discloses everything as applied to Claim 4 above. Mittra also discloses that communications must include a signature in order to verify the message (column 7, lines 60-63); however, Mittra does not explicitly disclose the relationship used to verify the signature. Schneier discloses that public key cryptography can be used for digitally signing documents. Specifically, a signature is formed by encrypting a document with the sender's private key, and the signature is verified by the receiver by decrypting the document with the sender's public key (page 37, "Signing Documents with Public-Key Cryptography", where the document corresponds to  $Z(A)$ , the public key corresponds to  $pAD$ , and the private key corresponds to  $sAD$ ). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification taught by Schneier in the authentication method of Mittra, in order to allow the signature to be authentic, unforgeable, and usable only once (see Schneier, page 37).

In reference to Claims 8 and 10, Mittra discloses a method for authenticating key devices, in which each key device is assigned a device-specific certificate (column 11, lines 35-38), including the steps of assigning each device a group-specific public key, where the group is comprised of a limited total number of key devices (column 8, lines 15-35; column 9, lines 56-58); assigning each key device a group-specific signature of its certificate (column 11, lines 35-39); establishing a link between at least two key devices; transmitting a corresponding device-specific certificate and signature from one of the key devices to another of the key devices (column 11, lines 35-41, where the signed certificates are sent along with any message sent to the group); and verifying authenticity of the corresponding device-specific certificate using the corresponding public key (column 11, lines 8-10). Mittra also discloses that communications must include a signature in order to verify the message (column 7, lines 60-63); however, Mittra does not explicitly disclose the relationship used to verify the signature.

Schneier discloses that public key cryptography can be used for digitally signing documents. Specifically, a signature is formed by encrypting a document with the sender's private key, and the signature is verified by the receiver by decrypting the document with the sender's public key (page 37, "Signing Documents with Public-Key Cryptography", where the document corresponds to  $Z(A)$ , the public key corresponds to  $pAD$ , and the private key corresponds to  $sAD$ ). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification taught by Schneier in the authentication method of Mittra, in order to allow

the signature to be authentic, unforgeable, and usable only once (see Schneier, page 37).

In reference to Claim 11, Mitra further discloses that the public key and signature are allocated during a first initialization (column 8, lines 33-35).

In reference to Claim 12, Mitra further discloses that each key device is compared with a stored list of approved key devices (column 7, lines 52-57).

### ***Conclusion***

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

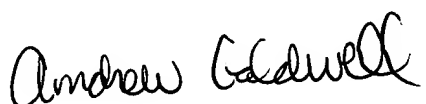
A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
zad

  
**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**